Report No. 2008-21

July 15, 2008

Department of Administrative Services: State Data Center Review

Bill Bradbury, Secretary of State

Charles A. Hibner, Director, Audits Division

Secretary of State Audit Report

Summary

PURPOSE

The Department of Administrative Services (department) is responsible for providing centralized services to state agencies, including computer networks and processing infrastructure. During 2005, the Oregon State Legislature approved funding for the Computing and Networking Infrastructure Consolidation (CNIC) project to consolidate 12 state agency data centers into one facility.

The primary purpose of this audit was to evaluate the status of the department's efforts to reengineer the State Data Center (SDC) environment to achieve CNIC project objectives. In addition, because of the criticality of SDC operations, we also evaluated controls governing the current SDC computing environment.

RESULTS IN BRIEF

Based on our audit work we found:

- Important data center consolidation objectives have not yet been achieved. As a result, it is unlikely that the anticipated savings or operational benefits associated with the CNIC project, such as enhanced enterprise disaster recovery and security solutions, will occur.
- Operational controls did not sufficiently address service level agreements with customers, performance and capacity management, standard operating procedures, configuration management, or software licensing requirements.
- The department was ill-prepared to timely resume data center operations or assist agencies in their efforts to restore critical computer applications after a major disruption.
- The department had not provided a secure computing environment for SDC clients.

Because of the sensitive nature of system security, we issued a separate report to communicate findings and recommendations in accordance with ORS 192.501 (23), which exempts such information from public disclosure.

RECOMMENDATIONS

We recommend that the department:

- establish an appropriate project management framework and allocate resources to ensure data center consolidation objectives occur, including detailed plans directing how, when, and to what degree it will consolidate network servers, system tools, mainframe operations and operating system platforms;
- allocate resources to ensure the SDC gains full operational control, formalizes service level agreements with agencies, establishes standard operating procedures, provides performance and capacity management, implements a centralized configuration management system, and ensures controls to track system software licenses;
- create and test disaster recovery plans to ensure timely restoration of SDC infrastructure and systems, and coordinate and formalize disaster recovery plans for mission critical applications; and
- implement recommendations included in our confidential security report.

AGENCY'S RESPONSE

The Department of Administrative Services partially agrees with the recommendations. The department's response is attached to this report, beginning on page 6.

Background

The Department of Administrative Services (department) is responsible for providing centralized services to state agencies, including computer networks and processing infrastructure. State statute specifically directs the department to coordinate statewide planning and activities related to the acquisition, installation and use of all information and telecommunications technology for the state.

During 2005, the Oregon State Legislature approved funding for the Computing and Networking Infrastructure Consolidation (CNIC) project to consolidate twelve state agency data centers into one facility. The total cost of this project was projected to be approximately $63.6 million, consisting of approximately $20 million to construct a new data center building and $43.6 million to equip and configure the consolidated operating environment. The project was intended to reduce future costs while maintaining or improving service levels.

In September 2006, the Oregon Audits Division completed an initial risk assessment of the CNIC project. The resulting report, *Department of Administrative Services: Computing and Networking Infrastructure Consolidation (CNIC) Risk Assessment*, identified several weaknesses in the department's project planning and management processes that adversely affected the integrity and viability of the project.

In response, department managers agreed that initial project planning and management was inadequate. They further indicated they would correct the deficiencies identified in the report by generally improving identified weaknesses and by reengineering the environment after agencies relocated to the State Data Center (SDC).

By the beginning of 2007, 11 agencies had transferred their data center operations to the department's SDC. Those operations include statewide enterprise applications and critical agency applications.

The primary purpose of this audit was to evaluate the status of the department's efforts to reengineer the SDC environment to achieve original CNIC project objectives. In addition, because of the criticality of SDC operations, another purpose was to evaluate the controls governing the SDC computing environment. Specifically, we chose to evaluate established controls over data center operations, disaster recovery, and security.

Audit Results

Significant Data Center Consolidation Objectives Have Not Yet Been Achieved

As outlined in our previous audit report, an effective project management framework is necessary to provide clear direction regarding project scope and boundaries. It also provides a roadmap for successful project completion and closure. In addition, project plans should be in place that detail how major objectives will be achieved.

At the conclusion of our previous audit of the CNIC project, agency managers were in process of moving their data center infrastructure and operations to the SDC. At that time, department managers had not yet developed comprehensive plans to achieve project objectives. Instead, they opted to relocate agency data centers to the SDC in their "as-is" state, stabilize operations, and then proceed with projects to reengineer the environment.

During this audit, we evaluated the department's efforts to resolve data center consolidation issues and to reengineer the SDC environment. Based on the results of this work, we concluded that important data center consolidation objectives had not yet been achieved. Specifically, the department had not made significant progress toward:

- defining the detailed end-state architecture of the SDC;
- reducing the number of network servers or operating system platforms;
- providing additional enhanced enterprise disaster recovery or security services for SDC clients;
- reducing SDC staffing levels; and
- consolidating data center operating procedures.

In addition, some agencies were unable to successfully relocate their operations to the SDC. In fact, at the conclusion of this audit, SDC managers indicated they will be moving approximately 200 network servers out of the SDC because it currently does not have sufficient power capacity to safely host those servers. The department indicated the above power issue was a transitory condition that would be resolved by consolidating the server environment through virtualization. However, we noted the department did not have a definitive plan to achieve this goal.

Furthermore, the Department of Education's data center did not participate in the data center migration as originally planned. Its move was delayed pending resolution of potential legal questions regarding confidentiality of student records. In light of the SDC power capacity problems mentioned above, we concluded movement of the Department of Education's data center to the SDC would likely be infeasible.

The above consolidation issues existed because the department continued to lack an appropriate project management framework. Components of that framework that were noticeably absent included:

- a dedicated management structure that was responsible for governing overall consolidation efforts;
- project plans defining how, when, or to what degree CNIC project objectives would, or could, be achieved; and
- sufficient dedicated resources, including the necessary staffing, to resolve the above issues or achieve intended results.

The overall effect of not achieving CNIC objectives is significant. Justification for the project centered on anticipated cost savings and operating efficiencies to be achieved by consolidating data center infrastructure, operations and human resources. If consolidation does not occur, it is unlikely that actual cost savings can be achieved to allow the department to recoup its CNIC investment of approximately $63.6 million. In addition, promises of increased operational benefits such as enterprise disaster recovery and security solutions will likely not materialize.

We recommend that department management establish an appropriate project management framework, and allocate resources, to ensure that data center consolidation objectives occur within the current SDC environment. That framework should include detailed plans directing how, when, and to what degree the SDC will consolidate network servers, system tools, mainframe operations and operating system platforms.

Agency's Response:

The department's response is attached to this report, beginning on page 6.

Some State Data Center Operations Were Not Uniformly or Effectively Controlled

Providing a controlled and stable operating environment for an enterprise data center includes managing basic Information Technology (IT) support functions such as:

- responding to customer needs and requests,
- resolving incidents and problems,
- establishing service-level agreements with customers,
- scheduling and prioritizing jobs and processes,
- managing and monitoring performance and capacity,
- managing the configuration, and
- ensuring compliance with outside requirements.

We found that the SDC had various processes for responding to customer needs. These controls included establishing a service desk to provide customer support, manage incidents, and receive service requests. The SDC also manned a command center to monitor the status of operating systems, jobs in progress, and network device status. In addition, it had processes to track the status of service tickets, change orders, and support requests. However, the SDC had not:

- established comprehensive service-level agreements with its agency customers;
- developed standard operating procedures for job scheduling, backup, and tape management;
- established a planning process for review or resolution of performance and capacity management issues;
- developed processes to manage the configuration of SDC infrastructure; and
- implemented controls to ensure compliance with software licensing requirements.

These issues existed primarily because the department did not have sufficient resources or the managerial structure to appropriately resolve them. As we previously discussed, the department chose to move agencies into the data center in their "as is" state, with the intent that SDC staff would subsequently reengineer the environment. However, since migration, SDC management has focused resources on providing ongoing services to customers. As such, staff has not been available to establish new data center controls, such as developing a comprehensive configuration management system. In addition, some operational requirements, such as establishing service-level agreements and standard operating procedures, remained undeveloped because SDC management had not assumed operational control of some agency platforms or established consensus with application owners regarding operating requirements and expectations.

The weaknesses noted above directly affected the SDC's ability to provide necessary and cost-effective services to its clients. For example, configuration management weaknesses affected the SDC's ability to develop and implement effective disaster recovery plans. In addition, configuration and capacity management issues inhibited efforts to consolidate SDC systems and resources. Furthermore, without formal service level agreements, the department and its customers remained uncertain regarding how critical operating requirements would be fulfilled.

We recommend department management allocate appropriate

resources to develop and implement controls to:

- ensure full control of the SDC operating environment and establish consensus with system owners, via formal service level agreements, regarding operating requirements and expectations;
- establish standard operating procedures for job scheduling, backup, and tape management;
- plan for and resolve performance and capacity management issues;
- maintain a centralized configuration management system to document important information regarding the operating environment; and
- track software licenses.

Agency's Response:

The department's response is attached to this report, beginning on page 6.

The SDC Lacked Appropriate Disaster Recovery Plans

The SDC hosts numerous mission critical computer applications, as well as enterprise Information Technology (IT) infrastructure. Therefore, department management is responsible for ensuring that data center infrastructure, including networks, operating system environments, and data storage facilities, can be timely restored in the event of a disaster or other major incident. In addition, the department shares the responsibility for coordinating and prioritizing the restoration efforts for agency computer applications hosted at the SDC with business owners.

Generally accepted controls suggest that organizations have formal continuity plans that mitigate the business risks associated with a major disruption or loss of IT services. Those plans should contain detailed response and recovery procedures to timely bring the business back to its "before-incident" state. Continuity plans should also be periodically updated and tested to ensure their viability. Because the SDC is a service provider, it should establish formal service level agreements with its customers to clarify and coordinate disaster recovery responsibilities and expectations. Those agreements should define each party's specific expectations during a recovery effort, and should address critical issues such as staffing, required recovery timelines and resource allocation.

We evaluated the SDC's controls over disaster recovery. Based on that work, we concluded the SDC was ill-prepared to timely resume data center operations or assist agencies in restoring their critical computer applications after a major disruption.

Items of most concern included the following:

- The SDC did not have formal or complete business continuity or disaster recovery plans for its operating systems, networks, data storage systems, or system utilities.
- SDC staff had not tested existing disaster recovery strategies.
- The department had no formal service level agreements with agencies addressing their disaster recovery needs, requirements or expectations.

Our prior audits of the state's major data centers and critical computer applications identified insufficient disaster recovery planning as a weakness. CNIC project planners also identified insufficient disaster recovery planning as a significant project risk. Based on the results of this audit, these conditions have not significantly changed. We concluded that these findings continued to exist because the department had not placed sufficient priority, or allocated sufficient resources, to resolve them.

We recommend that department management assign a higher priority to disaster recovery by allocating sufficient resources to create and test disaster recovery plans to ensure timely restoration of the SDC operating environment. Those plans should also ensure that SDC efforts are coordinated with agency expectations and requirements to recover mission critical computer applications hosted at the SDC. The plans should be formalized through service-level agreements.

Agency's Response:

The department's response is attached to this report, beginning on page 6.

The Department Did Not Provide For a Secure Computing Environment

The department is responsible for overall security of the SDC and for providing various other security services at the enterprise level. These responsibilities include but are not limited to:

- ensuring physical and logical security of SDC resources;
- monitoring state network traffic to identify, and react to, security threats;
- conducting vulnerability assessments of agency information systems; and
- establishing a state information systems security plan and associated standards, policies and procedures.

We evaluated the department's efforts to address these responsibilities and concluded that the department had not provided a secure computing environment for SDC clients.

Because of the sensitive nature of system security, we have issued a separate report outlining specific details of our findings, as well as

recommendations to improve security. That confidential report was prepared in accordance with ORS 192.501 (23), which exempts such information from public disclosure.

We recommend that department management implement the recommendations included in our confidential report.

Agency's Response:

The department's response is attached to this report, beginning on page 6.

Objectives, Scope and Methodology

The purpose of our audit was to evaluate the status of consolidation and the general computing controls at the State Data Center. Our specific audit objectives were:

1. Determine the status of consolidation.
2. Determine whether the department had implemented general computing controls to ensure continuous service by the State Data Center as required in the event of a disruption.
3. Determine whether the department had implemented general computing controls to ensure the State Data Center provided a stable and controlled operating environment.
4. Determine whether the department had ensured system security of State Data Center operations by maintaining the integrity of information and processing infrastructure, and minimizing the impact of security vulnerabilities and incidents.

To achieve these objectives, we interviewed various department personnel, observed operations processes, reviewed department documentation, and conducted tests. Tests included review of logical access, evaluation of project planning documents, and verification of the existence of supporting documentation.

We also reviewed the status of the findings and recommendations from our prior risk assessment of CNIC that were relevant to our current audit objectives.

We used the IT Governance Institute's (ITGI) publication, "Control Objectives for Information and Related Technology," (CobiT) to identify generally accepted and applicable interim control objectives and practices for information systems.

We conducted our audit according to generally accepted government auditing standards.

Oregon
Theodore R. Kulongoski, Governor

Department of Administrative Services
Office of the Director
155 Cottage Street NE, U20
Salem, OR 97301-3966
(503) 378-3104
FAX (503) 373-7643

July 3, 2008

Neal E. Weatherspoon, CPA, CISA, CISSP
Audit Manager, Audits Division
Office of the Secretary of State
255 Capitol Street NE, Suite 500
Salem, OR 97310

Re: State Data Center Review

Dear Mr. Weatherspoon:

Thank you for providing us the draft report regarding the State Data Center Review on April 22, 2008. We appreciate the time and effort your team has spent reviewing this program over the last 11 months. The Department of Administrative Services (Department) partially agrees with the findings as stated in the report and offers the following in response.

The draft report addresses four areas for improvement within the Department's State Data Center (SDC) operations. These areas include achievement of consolidation objectives, operational controls, appropriate disaster recovery plans and providing for a secure computing environment.

Significant Data Center Consolidation Objectives Have Not Yet Been Achieved
Management agrees that much work remains to achieve the goals of the consolidation. It is important to note that consolidating the State of Oregon's information technology (IT) infrastructure is a five year effort. The plan to re-architect and re-engineer Oregon's information technology requires a complex and interrelated set of plans to re-engineer 30 years of accumulated infrastructure. The SDC has developed an exhaustive process and technology architectural blueprint as well as associated standards. The complex migration from an unplanned ad-hoc structure to the blueprint must be implemented slowly, deliberately, and with adequate testing and impact analysis.

Since the audit was conducted the SDC has completed several projects for consolidation, many of which address findings in the audit report. Recently completed projects and those scheduled to be completed by year end 2008 can be found in Appendix A.

The report also addresses three areas in which components of an appropriate project management framework were noticeably absent:

> **A dedicated management structure that was responsible for governing overall consolidation efforts**
> It certainly would facilitate consolidation projects if two management structures and associated resources were separated and assigned to operations and consolidation. The SDC has four project managers down from ten that existed during the Computing and Networking Infrastructure Consolidation (CNIC) phase. The decrease is due to the elimination of project management headcount within the Department and the practicality to increase SDC project management resources at the cost of operational resources. Financial and human resources are allocated first to agency business requirements limiting the availability of funds and people

for consolidation projects. The SDC governing boards have opted for system consolidation to occur over the next five years as hardware is retired and replaced with new technology.

A new governance model for the SDC has recently been established. Since the audit was conducted, the Chief Information Officers (CIO) and agency directors have agreed in principle to the charter, composition, and responsibilities of the SDC Advisory Board, the SDC CIO Board, the SDC Finance Committee and the CIO Management Council. These governing boards are in the final stages of memorializing governance processes for:

- Scope Exclusion/Inclusion;
- Project Oversight;
- Financial and Billing Oversight;
- Staffing and Resource Management;
- Project Review and Associated Prioritization Processes; and
- Standards Exceptions.

Project plans defining how, when, or to what degree CNIC project objectives would, or could, be achieved

We agree that much work remains to standardize, streamline, and consolidate the State's Data Center. With our agency customer's daily operations taking precedence over consolidation, it is reasonable to expect such a massive re-engineering project to take many years to achieve stated objectives. We are managing to a plan which describes the future state objectives, outcomes, benefits and the implications associated with failure to reach part or all of a future state outcome over the span of five years. Some of the consolidation achievements that have been implemented, with benefits realized are included in Appendix A.

Sufficient dedicated resources, including the necessary staffing, to achieve intended results

Management does not believe having additional resources dedicated to consolidation would have a significant effect on the time to implement associated projects. The reason being, many of the enterprise management concepts and implementation plans require skills and experience that does not currently exist in state government. Therefore, we are heavily reliant on the procurement and management of third party system integrators with enterprise data center consolidation experience to assist with plan implementation. Such reliance is subject to the constraints of the procurement process and the funding levels available in the SDC budget.

Further, implementing the blueprint must be done without disruption to agency business operations. Migration workload must be coordinated and balanced with the operational workload of the SDC and that of agency programming staff. When considering critical business processes and the associated operational workload, it is prudent to prioritize the operations of government higher than data center consolidation projects. Resources are thus allocated according to this prioritization.

The report further addresses cost concerns, noting that: **If consolidation does not occur, it is unlikely that actual cost savings can be achieved to allow the Department to recoup its CNIC investment of approximately $63.6 million. In addition, promises of increased operational benefits such as enterprise disaster recovery and security solutions will likely not materialize.**

Cost savings is simply old base costs of IT less the current costs of IT for the same base and the same level of service. The difficulty in quantifying savings to the State of Oregon is due to:

- Detailed audits and analysis were not performed to verify total data center costs reported by the agencies in 2004; and
- Costs were reported in 2004 prior to a detailed specification of the requirements, scope of service, service levels, and computing growth trends and inflation. Since that time computing capacity and scope of services for the SDC have grown substantially.

The SDC has compared various rates it charges with identical services from other states. In almost all cases, the Oregon SDC rates are amongst the lowest published rates from other State Data Centers. Furthermore, when using industry standard ratios for staffing and for data center costs as a percentage of total information service expenditures, once again the Oregon SDC compares quite favorably as a low cost provider of data center services. It is also interesting to note that, for Department IT customers prior to the SDC, where costs and scope were known, base costs of computing have actually decreased by 12 percent since the SDC was implemented.

Some State Data Center Operations Were Not Uniformly or Effectively Controlled

We agree that at the time all systems were moved into the SDC, enterprise management processes and controls, where they existed, were inadequate to support the scale and complexity of the SDC. Many important processes and controls simply did not exist in the agency data centers prior to consolidation. Those that did exist were tailored to the unique work flows and processes of a particular agency. In no case were any processes integrated into an enterprise-wide work flow. Implementing enterprise processes is a long term project, requiring work force education, integration with agency business processes, customer testing and acceptance, as well as tool implementation. Following International Technology Infrastructure Library (ITIL), a framework of generally accepted data center process management and controls, the SDC has created a vision, blueprint, and plans for implementation. The SDC has decided to implement ITIL, a component at a time, starting with the most critical processes. At the time each component is implemented it is then integrated with previously implemented components resulting in comprehensive workflow. Such an implementation constitutes the core of the re-engineering of IT for the state.

While not at the maturity level the SDC plans for in the future, interim processes for change, problems, incident management as well as customer support have been implemented. Currently, the SDC is enhancing those processes and automating them by implementing an open source system scheduled to be completed by year end 2008. That web based system (entitled S3), will add to the above processes, assets and configuration management.

Processes such as system/network fault monitoring, capacity, and performance management have been slow to be implemented due to significant technical and architecture constraints of the State's pre-existing computing environment. Recently, and with the help of outside contractors, the SDC has architected, and is in the process of implementing, a technical work around for these obstacles. For security reasons, we cannot discuss the solution in this report. However, by the end of 2008, the SDC plans to have completed a comprehensive and integrated system for managing service levels, capacity, and performance across all domains.

The SDC Lacked Appropriate Disaster Recovery Plans

Management agrees that disaster recovery plans are inadequate and need corrective action. Since the audit, the SDC has conducted a detailed analysis of deficiencies in disaster recovery and is in the process of implementing the recommendations. Additionally, agencies have identified their critical

applications and recovery time objectives. The SDC is also implementing software tools that will map the agency identified applications with the associated infrastructure thereby facilitating effective disaster planning. We expect to have a fully tested data center disaster recovery plan in place by year end 2008.

The Department Did Not Provide For a Secure Computing Environment
Management partially agrees with this finding. Due to the highly confidential nature of security, the Department will respond in a separate and confidential document.

The Department appreciates the audit team's help in analyzing and discussing the important issues at the SDC. SDC staff believe they are prepared to achieve better business results and additional savings in the future based on these findings. If you have any further questions, please do not hesitate to contact Mark Reyer, SDC Administrator, at (503) 378-6430 or mark.reyer@das.state.or.us.

Sincerely,

Scott L. Harra
Director
Department of Administrative Services

cc: Kris Kautz, DAS Deputy Director
Chuck Hibner, Oregon Audits Division Director
Mark Reyer, State Data Center Administrator
Julie Bozzi, State Data Center Deputy Administrator
Pamela J. Stroebel Valencia, Chief Audit Executive

attachment

Appendix A
SDC Progress Completed Post Secretary of State Audit

Recently Completed Projects

1. The end-state for the consolidated data center has been developed and documented. These blueprints include comprehensive system architecture, technology standards, and thorough end-to-end IT System Management processes;
2. A five year SDC roadmap is available;
3. All systems and devices are monitored 24 hours a day, seven days a week through a recently implemented monitoring system;
4. Phase one of the network consolidation is complete;
5. System availability is reported monthly to SDC customers;
6. Approximately 70 servers have been eliminated;
7. Project plans are available for the next nine to 12 months of consolidation activities;
8. Server standardization and consolidation will continue over the next five years as servers are retired and customer agencies can be supported with standard and virtualized technology; and
9. A new software license management system has been implemented. It will be integrated into the enterprise asset management system as indicated below.

Current Projects (scheduled to be completed by year end 2008)

1. Software systems are currently being implemented to report on capacity and utilization of all SDC infrastructure including servers, network devices, and storage.
2. Multiple mainframes are being consolidated on to a single mainframe.
3. Over 100 mid-range computers are being consolidated onto two IBM midrange systems.
4. Tools and analysis will be completed on unused and low-used software that can be removed or consolidated on SDC systems.
5. A single storage management and backup/recovery system will be complete by year end 2008. This will replace 11 different processes, utilizing 20 separate software packages, across 24 different hardware platforms.
6. A unified IT lifecycle and workflow systems encompassing request management, asset management, licensing, configuration management, service level reporting, change and incident management is scheduled to be complete by year end 2008. This will create a single workflow for SDC and its customers replacing dozens of incongruent systems and processes.
7. All network applications are scheduled be centralized from 18 servers onto a single appliance system by October 2008.
8. Firewall consolidation and standardization is scheduled to be complete by year end 2008.
9. Server standardization and consolidation will continue over the next five years as servers are retired and Agency customers can be supported with standard and virtualized technology.
10. Scope of Services provided by the data center is in its final negotiations with agency customers and the SDC. It is anticipated that service scope will be finalized and accepted by the SDC governing boards within the next 30 days.
11. Upon completion of the scope agreement, the SDC along with the customer will develop comprehensive service levels for those services in scope. It is expected that this will be completed within 90 days after agreement of the scope agreement.
12. The SDC has reached agreement on a standard process for job scheduling, backup/recovery, and tape management with the agency customers. The standard job scheduling process is scheduled to be implemented within the next 90 days. The standard backup/recovery and tape management process is scheduled to be implemented with the implementation of a single storage management system as indicated above by year end 2008.

Secretary of State
Audits Division

255 Capitol St. NE, Suite 500
Salem, OR 97310

Auditing to Protect the Public Interest and Improve Oregon Government

AUDIT MANAGER: *Neal E. Weatherspoon, CPA, CISA, CISSP*

AUDIT STAFF: *Erika A. Ungern, CISA*
Constance S. Bailey

DEPUTY DIRECTOR: *William K. Garber, CGFM*

Courtesies and cooperation extended by officials and staff of the Department of Administrative Services were commendable and much appreciated.

This report, a public record, is intended to promote the best possible management of public resources. Copies may be obtained:

Internet: *http://www.sos.state.or.us/audits/index.html*

Phone: *at 503-986-2255*

Mail: *Oregon Audits Division*
255 Capitol Street NE, Suite 500
Salem, OR 97310